



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/824,930

04/15/2004

Thomas A. Gentles

1842.047US1

7285

70648

7590

03/24/2008

SCHWEGMAN, LUNDBERG & WOESSNER/WMS GAMING

P.O. BOX 2938

MINNEAPOLIS, MN 55402

EXAMINER

KIM, ANDREW

ART UNIT

PAPER NUMBER

3714

MAIL DATE

DELIVERY MODE

03/24/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.



## **DETAILED ACTION**

### ***Response to Amendment***

This office action is in response to the amendment filed on 12/13/07 in which:

- Claim(s) 1.3.10.12.23.24.25 have/has been amended.
- Claim(s) 19 have/has been canceled.
- Claim(s) 26-28 have/has been added.
- Response to claims rejection have been filed.
- Claim(s) 1-18, 20-28 are pending.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

**Claims 1-18, and 20-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Martinek et al. (US 7,043,641), "Martinek".**

Claim 1. Martinek discloses a method performed by a gaming system server, the method comprising: authenticating a gaming terminal's identity (col. 10:19-27);

When the gaming terminal's identity is authenticated, then:

applying an encryption technique to encrypt a gaming software program, which produces an encrypted gaming software program (abstract, col. 6, 8:52-64); and

transmitting the encrypted gaming software program to the gaming terminal (abstract, col. 6).

Martinek substantially discloses the invention as claimed but fails to explicitly teach that the encryption technique is applied after authentication. Instead, Martinek discloses authentication of the gaming terminals and encryption in data in no set order. However, it would have been obvious to one of ordinary skill in the art at the time of the invention to first authenticate a terminal then encrypt the data for transmission. By ordering the steps in this manner, the server only uses valuable processing time encrypting data

Art Unit: 3714

requested by authenticated receivers. This reduces pointless processing and encrypting of data requested by an unauthenticated receiver because the data would not be sent to the unauthenticated receiver anyway. Therefore, one of ordinary skill in the art at the time of the invention would have found it obvious to first authenticate the gaming terminal before encrypting the data to save processing power and time.

Claim 2. Martinek discloses receiving a request to download the gaming software program from the gaming terminal (col. 5:41).

Claims 3 ,4. Martinek discloses wherein authenticating the gaming terminal's identity comprises: receiving a gaming terminal digital certificate from the gaming terminal (col. 6:1-23); and authenticating the gaming terminal's identity based on the gaming terminal digital certificate (col. 6, 10).

Claim 5. Martinek discloses generating a session key to use in applying the encryption technique (col. 6:1-23, 12:25-39).

Claim 6. Martinek discloses wherein the encryption technique is selected from a group of encryption techniques that includes a symmetric encryption technique and an asymmetric encryption technique (6:1-23, 10:19-39).

Claim 7. Martinek discloses wherein the symmetric encryption technique is an

encryption technique that uses a one-time session key (6:1-23, 10:19-39, 12:25-39).

Claim 8. Martinek discloses wherein the asymmetric encryption technique is selected from a group of asymmetric encryption techniques that includes a public key encryption technique, and a multiple-key public key encryption technique (col. 6).

Claim 9. Martinek discloses

establishing a public-private key-pair, which includes a public key and a private key (col. 6); and generating the gaming terminal digital certificate, which includes a digital certificate that is signed with the private key (col. 10:13-39).

Claim 10. Martinek discloses a method performed by a gaming terminal, the method comprising:

authenticating a gaming system server (col. 6:38-50);

when the gaming server's identity is authenticated (10:62-11:8)

receiving an encrypted gaming software program from the gaming system server (col. 6:38-50); and

applying a decryption technique to decrypt the encrypted gaming software program, which produces a gaming software program (fig. 4).

Claim 11. Martinek discloses sending a request to download the gaming software program to the gaming system server (col. 5:41).

Claim 12. Martinek discloses wherein authenticating the gaming system server's identity comprises: receiving a gaming system server digital certificate from the gaming system server; and authenticating the gaming system server's identity based on the gaming system server digital certificate (col. 6:38-50).

Claim 13. Martinek discloses wherein the decryption technique is selected from a group of decryption techniques that includes a symmetric decryption technique and an asymmetric decryption technique (col. 6:38-50).

Claim 14. Martinek discloses wherein the symmetric decryption technique is a decryption technique that uses a one-time session key (fig. 4 along with the related description).

Claim 15. Martinek discloses wherein the asymmetric decryption technique is selected from a group of asymmetric decryption techniques that includes a public key decryption technique, and a multiple-key public key decryption technique (col. 6).

Claim 16. Martinek discloses establishing a public-private key-pair, which includes a

public key and a private key; and generating the gaming system server digital certificate, which includes a digital certificate that is signed with the private key (col. 6, 10).

Claims 17-18, 21, 23-25. Martinek discloses a server of a gaming system generating a public-key private-key key pair; encrypting the public-key private-key key pair to produce an encrypted public-key private-key key pair; generating a certification authority digital certificate request, the certification authority digital certificate request including a public-key associated with the encrypted public-key private-key key pair; decrypting the public-key private-key key pair; and signing the certification authority digital certificate request using the private-key of the public-key private-key key pair to form the certification authority digital certificate (col. 6, 10, 11:36-48, 12:25-39).

Martinek substantially discloses the invention as claimed but fails to explicitly teach that the encryption technique is applied after authentication. Instead, Martinek discloses authentication of the gaming terminals and encryption in data in no set order. However, it would have been obvious to one of ordinary skill in the art at the time of the invention to first authenticate a terminal then encrypt the data for transmission. By ordering the steps in this manner, the server only uses valuable processing time encrypting data requested by authenticated receivers. This reduces pointless processing and encrypting of data requested by an unauthenticated receiver because the data would not be sent to the unauthenticated receiver anyway. Therefore, one of ordinary skill in



the art at the time of the invention would have found it obvious to first authenticate the gaming terminal before encrypting the data to save processing power and time.

Claims 20, 22. Martinek discloses a method comprising: receiving a first signed digital certificate from a server, the first signed digital having an associated first public-key private-key key pair and having a first digital signature from an approval authority, the first digital signature formed by digitally signing the first public-key of the first public-key private-key key pair with a first approval authority private-key from a first approval authority public-key private-key key pair; authenticating the server based on the first signed digital certificate.

Martinek substantially discloses the invention as claimed but fails to explicitly teach double encryption as claimed. Instead, Martinek teaches single encryption (abstract, col. 6) and authentication from both a regulatory agency and a game code manufacturer. However, One of ordinary skill in the art would have seen the benefit of modifying Martinek with double encryption to insure the security, authenticity, and validity of the data being exchanged between the gaming terminal and the gaming server. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the instant invention to modify Martinek with double encryption to insure privacy, authentication and validity.

Claim 26. Martinek discloses further comprising authenticating the gaming terminal digital certificate (11:36-48).

Claim 27. Martinek discloses further comprising authenticating the gaming server digital certificate (col. 11).

Claim 28. Martinek substantially the invention as claimed but fails to explicitly teach whether the gaming terminal is authorized to access the gaming software program comprises checking an access control list. However, it is old and well known in the security art to maintain an access control list when one wishes to restrict which certain computers should or should not connect to another computer (e.g. wireless routers has had this feature for a while).

### ***Response to Arguments***

Applicant's arguments filed 12/13/07 have been fully considered but they are not persuasive.

Applicant's arguments with respect to claims 1-18, 21, 23-25 have been considered but are moot in view of the new ground(s) of rejection.

Regarding claims 1, 23 and 24, see new grounds of rejection.

Regarding claims 10, 23, and 25, see new grounds of rejection.

Regarding claim 17, the encrypted public/private keys are disclosed in 10:19-11:8.

Regarding claim 18, the generations of digital certificates are disclosed in 10:19-11:8.

Regarding claim 21, Martinek discloses expiring signatures in 12:25-39.

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW KIM whose telephone number is (571)272-1691. The examiner can normally be reached on M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Xuan Thai can be reached on 571-272-7147. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.


Art Unit: 3714

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A.K. 3/26/2008

/XUAN M. THAI/

Supervisory Patent Examiner, Art Unit 3714

<div>Application Number</div> <div></div>	Application/Control No.	Applicant(s)/Patent under Reexamination	
	10/824,930	GENTLES ET AL.	
	Examiner	Art Unit	
	ANDREW KIM	3714	